GOTC

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPEN SOURCE , OPEN WORLD

「开源云原生计算时代」专场

助力企业安全拥抱云原生

张涛 2021年08月01日

企业数字化驱动应用架构的现代化变革

GOTC

2020年43.9%的国内用户已在生产环境中采纳容器技术，超过七成的国内用户已经或计划使用微服务架构进行业务开发部署

数据中心整合

·硬件抽象
·资源池化
·统一运维

IT支撑业务

数据中心云化

·计算、存储、网络、资源的虚拟化建设
·关键应用云化
·智能化运维
·资源交付自动化

IT服务业务

应用现代化

·容器化建设
·微服务架构变革
·云原生构建
·DevOps实现

IT驱动业务

从FireEye被入侵看信息安全攻防的体系化、国家化、武器化

GOTC

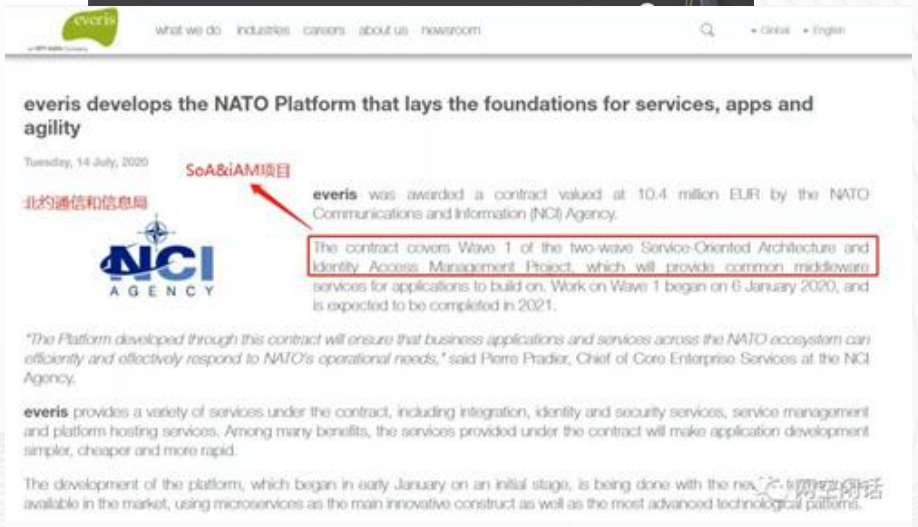
- 2020年12月8日，全球最大的网络安全公司之一FireEye（火眼）披露遭遇黑客入侵，黑客成功窃取了FireEye渗透测试客户网络的黑客工具RedEye，又被称为网络安全界的“核武泄露”。

- 虽然这次疑似国家级黑客组织花费巨大技术成本进行的APT攻击很可能是一场“赔本买卖”，但也预示着新一代信息技术的快速发展环境下，网络攻击愈发有组织，国家化甚至是武器化，大国网空博弈的战势从未被搁置，资金雄厚的对手暗潮涌动，网络空间防御时刻枕戈待旦。我们需要以新思路的、最优解的技术共同防御和应对资金雄厚的对手。

北约机密云平台遭到入侵

GOTC

- 2021 年 5 月，北约机密云平台的重要供应商Everis遭网络攻击，与云平台相关的重要代码、文档等数据全部失窃，攻击者勒索超10亿欧元赎金，甚至要把数据发给俄情报机构。
- 以下为DDoSecrets的报道：2021年5月，有黑客入侵一家名为Everis的西班牙企业及其位于南美洲的子公司，成功窃取多套数据集，包括与北约云计算平台相关的源代码及文档。除了拿到数据副本之外，黑客团伙还宣称已经删除了公司内的原始数据，并有能力修改代码内容甚至在项目中植入后门。攻击方还打算勒索Everis公司，甚至开玩笑称要把数据发送给俄罗斯情报部门。



everis develops the NATO Platform that lays the foundations for services, apps and agility

Tuesday, 14 July, 2020

SoA&iAM项目

北约通信和信息局

everis was awarded a contract valued at 10.4 million EUR by the NATO Communications and Information (NCI) Agency.

The contract covers Wave 1 of the two-wave Service-Oriented Architecture and Identity Access Management Project, which will provide common middleware services for applications to build on. Work on Wave 1 began on 6 January 2020, and is expected to be completed in 2021.

"The Platform developed through this contract will ensure that business applications and services across the NATO ecosystem can efficiently and effectively respond to NATO's operational needs," said Pierre Pradier, Chief of Core Enterprise Services at the NCI Agency.

everis provides a variety of services under the contract, including integration, identity and security services, service management and platform hosting services. Among many benefits, the services provided under the contract will make application development simpler, cheaper and more rapid.

The development of the platform, which began in early January on an initial stage, is being done with the nex... available in the market, using microservices as the main innovative construct as well as the most advanced technological platforms.

GOTC

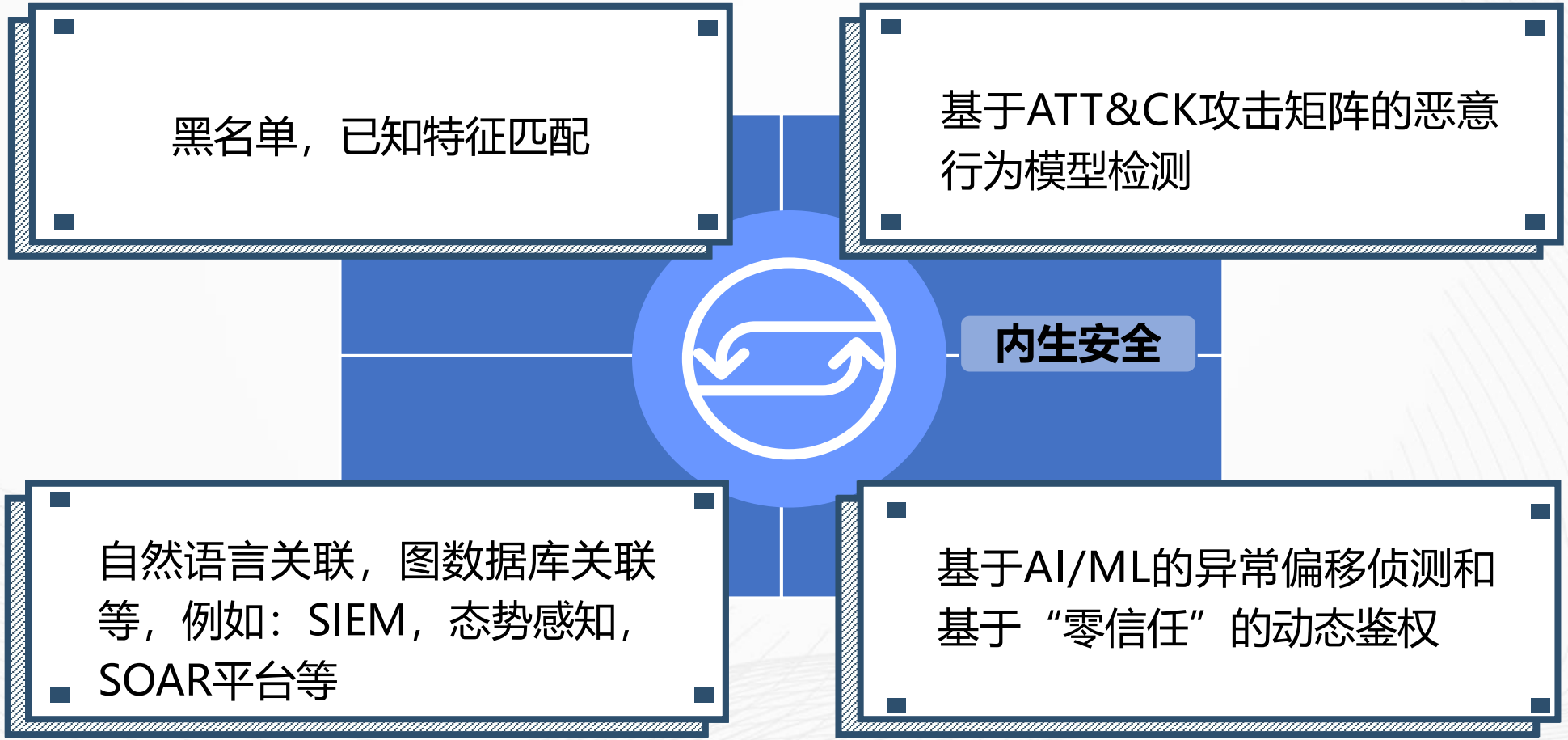
目录

CONTENTS

01
风险的“不确定性”

“黑天鹅和灰犀牛”

安全风险的“不确定性”


黑名单，已知特征匹配
基于ATT&CK攻击矩阵的恶意行为模型检测
内生安全
自然语言关联，图数据库关联等，例如：SIEM，态势感知，SOAR平台等
基于AI/ML的异常偏移侦测和基于“零信任”的动态鉴权

02

云原生安全设计理念

云原生带来的新的安全隐患

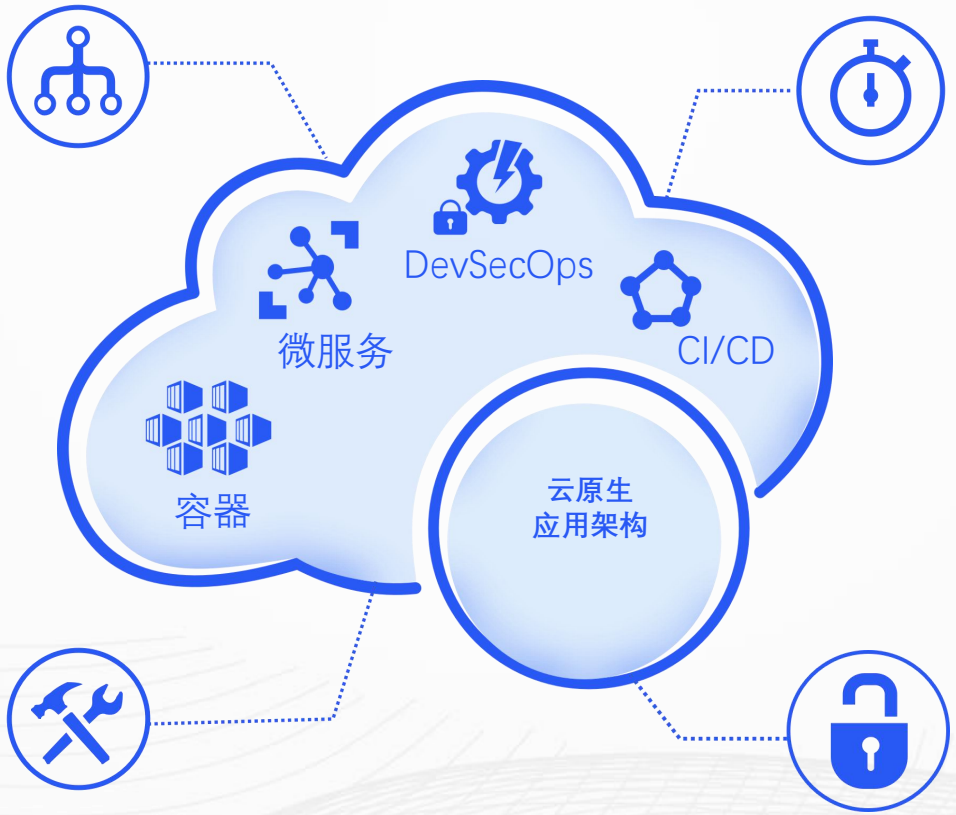
GOTC

传统的安全问题
在云原生环境依然存在

Web攻防和系统攻防，暴力破解和反弹Shell等问题依然存在，但传统工具无法工作在云原生环境中

运维管理流程和服务模型变化带来的管理难题

云原生资产风险深度可视化难题，DevSecOps流程难题，云服务商和企业的安全防护责任和边界不清晰等



云原生计算环境
引入新的安全风险

开发IDE安全，编排系统及组件安全，镜像及镜像仓库安全，容器网络安全，容器逃逸，运行时入侵

云原生化应用
引入新的安全风险

凭证泄露，微服务的攻击敞口及治理难度，Serverless模型安全，API爆炸产生的权限管控和资源滥用

03
云原生安全最佳实践

探真云原生安全方案

GOTC

云原生基础架构层安全-TensorCS

GOTC

安全左移

配置安全性及合规检查

代码安全扫描，静动态镜像和组件安全扫描

容行运行时安全

已知威胁的检测及防护

整合ATT&CK防御和以AI画像偏移侦测为依据的免疫防御

容器自动加固

嵌入CICD流程的自动化加固方案

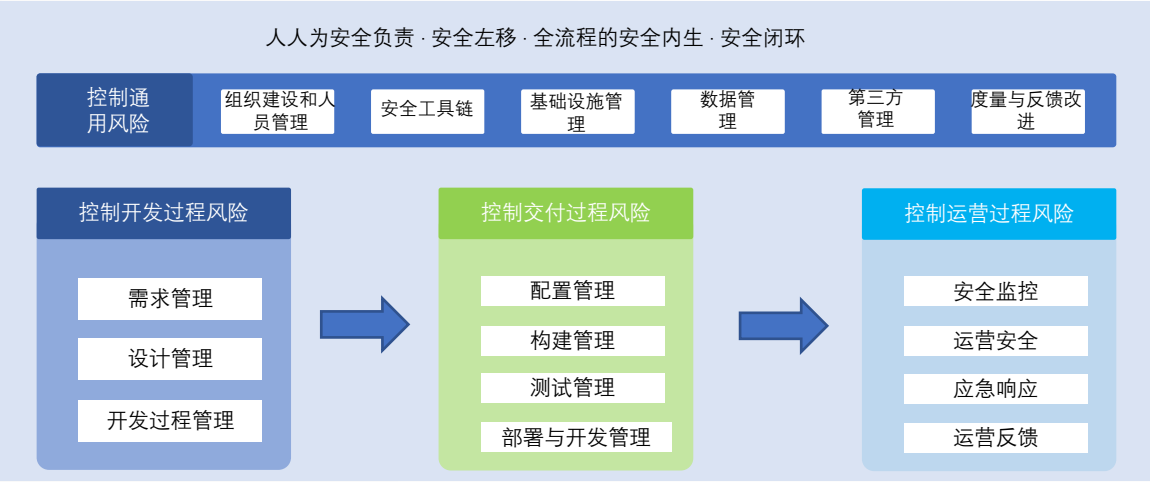
通过学习容器画像后自动加固容器

智能微隔离

智能容器环境网络隔离方案

基于流量学习的自动策略推荐能力

高效的云原生AISecOps能力演进



云原生安全能力

构建云原生安全能力，并这些安全能力自动嵌入CI/CD流程

镜像安全 | 容器加固 | 运行时安全
微隔离 | 动态鉴权 | WAF

云原生日志分析

基础设施/云/容器/应用的日志采集和分析，故障定位和实时告警

日志 | 大数据 | 实时告警
秒级检索 | 分析 | 可视化

泛安全大数据分析

资产漏洞、安全攻击事件、网络威胁情报、主机网络访问行为、容器访问行为等泛安全分析

安全态势 | 行为分析 | SOC
威胁情报 | ATT&CK | 资产

云原生智能运维中台

完整的系统指标监控
应用性能监控
故障解决和根因定位
高性能日志检索
全业务链故障跟踪
自动化运维平台
全维度运维工具链集成

日志 | 指标 | 监控 | APM
业务链 | 泛安全 | DevOps

AISecOps

在 DevOps 框架下，将安全防护机制贯穿至整个应用生命周期的每一个环节。
DevSecOps意味着从一开始就要考虑应用和基础架构的安全性，选择合适的工具集，持续集成安全防护，构建完整的应用全生命周期安全解决方案。

异常检测 | 聚类分析 | 预测
机器学习 | 智能响应 | 无人值守

云原生智能安全运维的支撑系统

GOTC

动态鉴权中心
基于角色权限，集中管理密码，密钥，证书

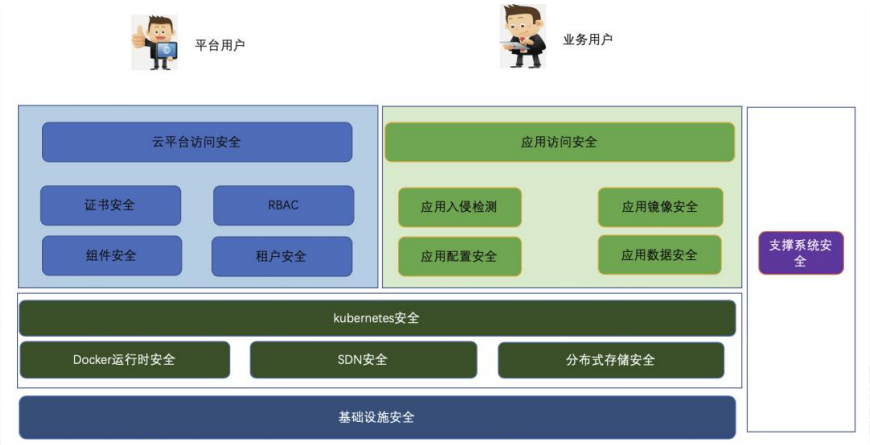
PAM
构建特权账号管理系统

CI/CD集成
安全能力自动嵌入CI/CD流程

RBAC
构建最小权限授权管理机制和强访问控制策略

UIMS/SSO
构建统一租户管理平台/构建统一身份认证平台

Audit
K8S api调用审计，管理平台用户操作审计



云原生安全方案最佳实践

GOTC

等保2.0一键对齐

检查所有云原生环境，帮助客户分析与等保2.0各级的差距，并通过解决方案满足等保相关技术要求

重要活动攻防对抗

帮助客户确保在红蓝对抗中，自动发现薄弱点，自动化加固容器，确保减少不必要的风险敞口和攻击通道

重要时期安全保障

基于操作系统内核级别的数据探测与服务级AI免疫画像技术，实时监控云原生环境运行状态，检测并防护已知和未知威胁

基于“零信任”的动态鉴权

业界领先的云原生应用动态鉴权方案，辅助客户完善软件开发流程以及大幅度增强安全性

了解更多

GOTC

微信搜索“探真科技”关注探真
获取最新云原生安全情报

全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

探真科技
TensorSecurity

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

探真科技
TensorSecurity